



Seattle Office of
Inspector General

Annual Surveillance Review: Technology Assisted Public Safety Pilot Program

As Required by Seattle Municipal Code 14.18.060

September 30, 2026

Office of Inspector General
City of Seattle
PO Box 94764
Seattle, WA 98124-7064

206.684.3663
oig@seattle.gov

Objective and Scope

The Office of Inspector General (OIG) is required by Seattle Municipal Code (SMC) 14.18 to review surveillance technologies used by the Seattle Police Department (SPD). This report is a review of 2025 use of Closed-Circuit Television (CCTV) Cameras, Fleetwide Automated License Plate Readers (ALPR), and the Real Time Crime Center (RTCC) software, implemented together as the Technology Assisted Public Safety (TAPS) Pilot Program. For each technology SMC 14.18 requires OIG to review usage patterns, data sharing, data management, risks to civil liberties and disproportionate impacts to disadvantaged populations, community concerns, and total cost.¹

Executive Summary

This initial annual review of TAPS pilot program technologies found that the Department implemented appropriate policies and processes to control the use of ALPR, CCTV, and RTCC software. RTCC staff and involved officers appeared to strictly limit use and sharing of information produced by the technologies to the investigation of crimes and incidents aligned with the stated priorities of the TAPS pilot program. This review found that SPD and City leadership did not sufficiently consider integration of private cameras in the development and approval of RTCC and CCTV Surveillance Impact Reports (SIRs) and should promptly identify appropriate guidelines. This review also identified that SPD should apply additional civil liberty safeguards by requiring authorized users to provide thorough justifications for any search in the CCTV or ALPR databases.

Acknowledgement

OIG wishes to express appreciation to SPD personnel, and specifically RTCC leadership, who assisted auditors with timely and complete access to information throughout this review. OIG is encouraged by the collaborative approach and thankful for the time they contributed.

¹ As requested by Mayor Harrel's Office in 2024, OIG is separately evaluating the effectiveness of TAPS in partnership with the University of Pennsylvania Crime and Justice Policy Lab, and that report is expected at the end of 2027. OIG is also aware of two concurrent reviews commissioned or performed by Mayor Wilson's office which address topics of cybersecurity and protections of surveillance data from external actors.

Contents

Real Time Crime Center (RTCC) and Closed-Circuit Television Cameras (CCTV)	4
How RTCC Analysts Use CCTV	6
Data Retention, Sharing, and System Access	12
Community Concerns and Costs	13
Automated License Plate Readers (ALPR)	15
How SPD Uses ALPRs	16
Data Retention, Sharing, and System Access	17
Community Concerns and Costs	21
Appendix A: SPD Management Recommendations Response	22

Real Time Crime Center (RTCC) and Closed-Circuit Television Cameras (CCTV)

Axon Fusus RTCC Software: a real-time intelligence and crime center platform that aggregates multiple data sources such as dispatch, camera footage, ALPR data, officer location, 911 calls, records management systems and visualizes them into a map view.

Real Time Crime Centers: specialized units within law enforcement agencies that integrate data from various sources with the goal of providing actionable intelligence and enhanced situational awareness to law enforcement in real-time.

In October 2024, City Council approved the implementation of Closed-Circuit Televisions (CCTV) cameras and the use of **Axon Fusus software** to establish a **Real Time Crime Center (RTCC)** within SPD. The descriptions of the technologies, the purpose of use, and other operational details are published in a document called a Surveillance Impact Report (SIR). While there are two separate SIRs for CCTV and RTCC, OIG reviewed these technologies together because their operations are interdependent.

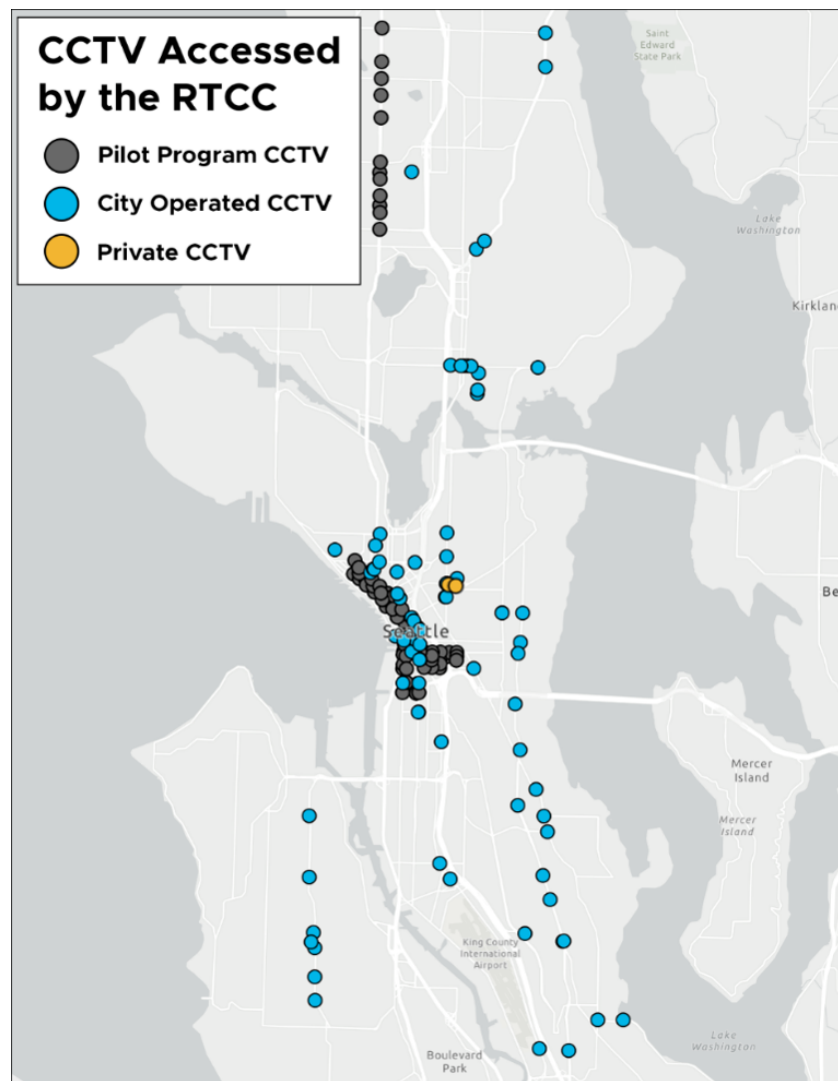


Figure 1. All CCTV Locations Integrated into the RTCC

In April 2025, SPD installed CCTV cameras at 62 locations and integrated them into the RTCC in three pilot areas: Chinatown-International District, Downtown, and Aurora.² In 2026, the Department installed cameras in 21 locations within the Stadium District and operated these while the City hosted FIFA World Cup matches. At the time of reporting the cameras in the Stadium District remain installed but are not operating.

Each pilot program CCTV location is operated by SPD. Each location is referred to as a “cabinet,” and includes five cameras: one for each cardinal direction (generally North, South, East, and West) and a pan-tilt-zoom (PTZ) camera. The cabinets also include the physical components involved in operating the cameras for data storage and transmission, called Fusus Cores. CCTV camera footage is approved for 30-day retention by the SIR, but in practice SPD opted to retain video for 5 days, unless it is identified for use in an investigation. In addition to 62 locations, SPD has also integrated Seattle Department of Public Transportation (SDOT), SPD Precinct Cameras, and privately-owned security systems, referred to as “private cameras” in this report, which are third-party cameras owned by a non-government entity such as a business. These camera streams are one of many data sources integrated into the Axon Fusus software that are used by RTCC analysts.

SPD policy allows RTCC analysts to view cameras only in response to a call or to assist an active investigation.³ Whenever RTCC analysts find camera footage relevant to an investigation, they create a clip of the footage or picture and save it to a cloud-based evidence repository called the Fusus Vault. RTCC analysts can then attach CCTV evidence from the Fusus Vault to a case number in Evidence.com.

2 The ordinance approving the SIR for CCTVs permits SPD to move cameras around within the approved neighborhood at any time.

3 SPD Policy [12.100-POL-4\(3\)](#).

How RTCC Analysts Use CCTV

RTCC Analysts Use CCTV to Support Investigations of Violent Crime and High-Priority Calls

The CCTV SIR states that “CCTV camera systems contribute to averting harm to individuals and property and reducing crime by assisting in collecting evidence related to serious and/or violent criminal activity as part of investigations.”

In 2025, RTCC analysts saved 1,659 clips of CCTV footage as evidence. OIG analyzed these and found that saved evidence generally aligned with the purpose statements in the SIR. As demonstrated in Figure 2, the vast majority (98%) of CCTV evidence was associated with high-priority calls or serious/violent crime as defined by the FBI’s National Incident-Based Reporting System.

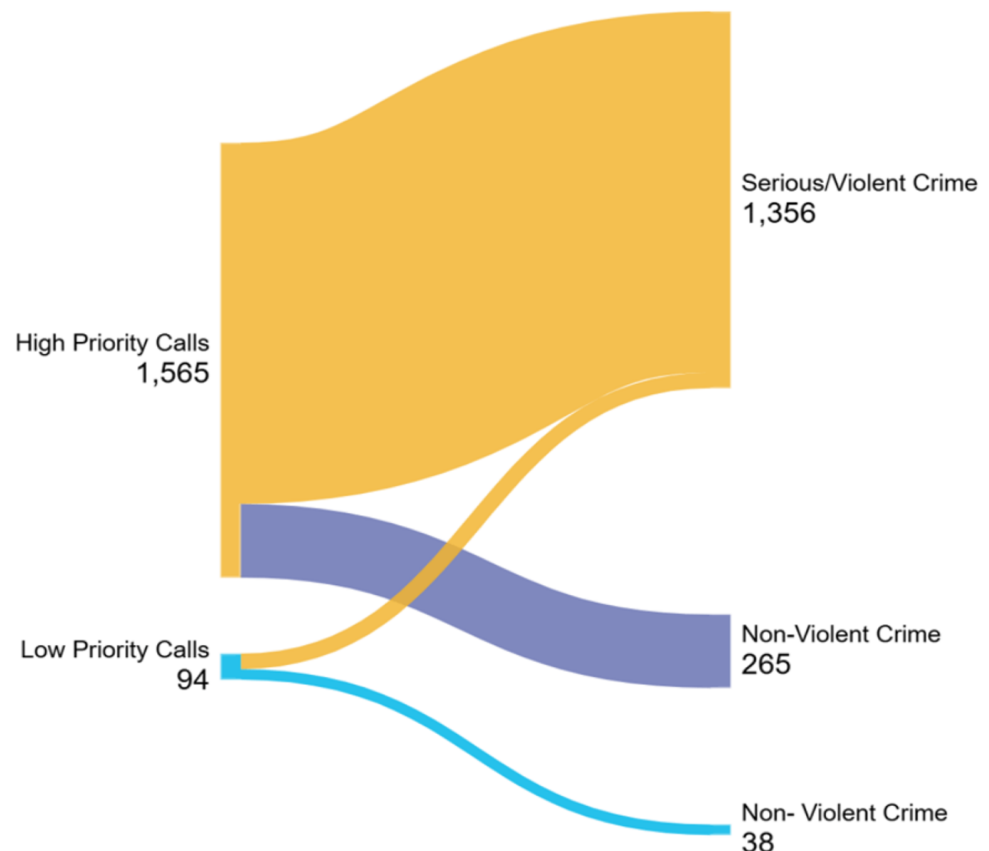


Figure 2. CCTV Evidence by Call and Crime Type

There were only 38 instances in 2025 where CCTV evidence was used to support incidents that were both non-violent and low-priority calls. Most of these involved an RTCC analyst assisting with traffic incidents.

SPD CCTV Cameras Do Not Use Facial Recognition Software

Facial recognition systems have been found to misidentify people of color and female faces more often, potentially leading to discriminatory impacts.⁴ Cities and localities, including King County, have banned the use of facial recognition technology because of the risk of misidentification, racial bias, and impact on civil liberties. In the City of Seattle, any use of facial recognition technology would require approval outlined in SMC 14.18.

The edge-based analytical capabilities of CCTV installed in Seattle do not include facial recognition software.⁵ These capabilities include object recognition such as cars, pants, hats, tops, bags, and people. This object recognition does not allow SPD to identify faces or persons based on demographic characteristics such as race, age, or gender. Instead, this feature detects objects and is used to identify things like the color of clothing. SPD reports that despite having object recognition capability, they do not often use this function because it can be inaccurate and/or time consuming.

SPD Prohibits RTCC Personnel from Proactively Monitoring CCTV

The National Institute of Justice (NIJ) outlines three monitoring functions of an RTCC: (1) focused policing, (2) real-time monitoring, and (3) investigations. Figure 3 demonstrates the range of RTCC monitoring functions from proactive to reactive.

4 National Institute of Standards and Technology, [Face Recognition Vendor Test Part 3: Demographic Effects](#), 2019; J. Buolamwini and T. Gebru, [Gender Shades: Intersectional Accuracy Disparities in Commercial Gender Classification](#), 2018.

5 Edge-based analytical capabilities refer to object recognition executed directly on the hardware device—in this context the camera or server, instead of in a centralized cloud data center.

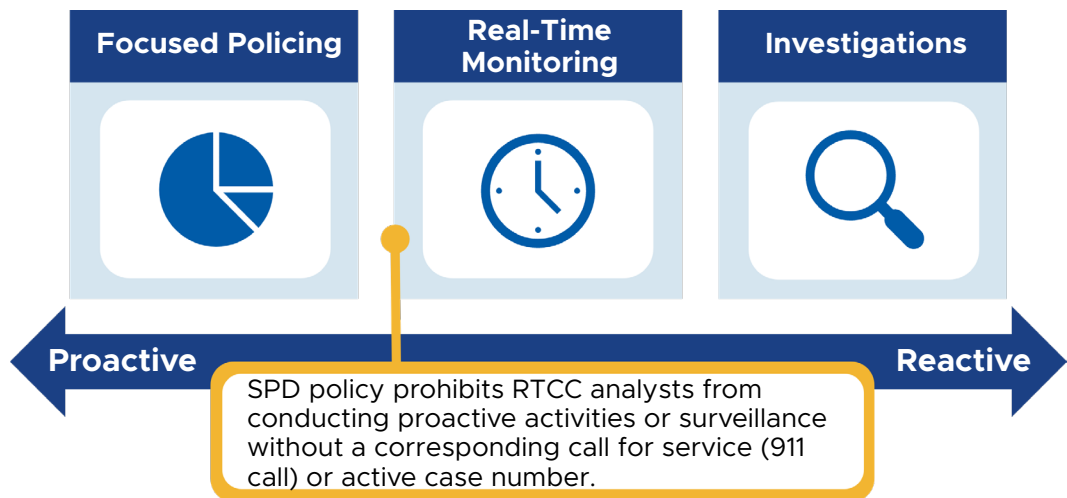


Figure 3. OIG generated graphic derived from the NIJ, Real-Time Crime Centers: Integrating Technology to Enhance Public Safety, 2025.

“Focused policing” methods use crime trends in historic police data to identify areas for law enforcement to proactively monitor. Because it is based on prior incidents and enforcement activities, focused policing can perpetuate bias by directing more police resources to already heavily policed neighborhoods.⁶

Responsive to the risk of proactive monitoring, SPD policy provides the following restriction on RTCC analysts:

“The RTCC will not independently access, log to, or participate in any ongoing investigation unless requested by authorized SPD personnel. They will not conduct proactive activities or surveillance without a corresponding call for service (911 call) or active case number.”⁷

While policy prohibits proactive surveillance, the Axon Fusus software does not currently have a process to prevent or monitor this kind of activity. RTCC personnel can view CCTV cameras without providing a justification such as a case number or CAD event. Absent this requirement, SPD lacks a way to prevent, control, or audit improper use of the technology.

SPD is making progress to improve controls in this area. In August 2026, SPD developed a strategy to track when RTCC analysts are logged to a call for service. Additionally, SPD has already met with Axon to discuss the future development of a search justification requirement to view camera footage.

⁶ National Institute of Justice, Real-Time Crime Centers: Integrating Technology to Enhance Public Safety, 2025.

⁷ SPD Policy [12.100](#).

Recommendation 1: Implement Additional Access Controls for Viewing CCTV Feeds

SPD should request Axon implement a requirement for RTCC analysts to provide a case number and/or justification for each instance they view CCTV camera footage in the Axon Fusus software.

SPD Digitally Masks Private Spaces Within View of SPD-Operated Cameras

To address privacy concerns, SPD policy states that prior to installation and during use of the technology SPD will:⁸

- Ensure CCTV technology only monitors public spaces such as sidewalks, streets, and parks.
- Apply permanent **digital masking** on cameras that have non-public spaces within their field of view, such as apartment building windows.⁹

Digital Masking: a security feature that blacks out certain areas in a camera's field of view to ensure the area is not visible or recorded.

Because SPD policy does not explicitly define allowable visibility into non-public spaces, OIG sought to understand how SPD implemented their policy on camera orientation and digital masking by reviewing more than 100 unique camera angles captured in evidence clippings. OIG found only five evidence clippings where non-public spaces such as apartment or hotel windows were visible from the street and might reasonably require masking. SPD confirmed two of the relevant cameras were currently masked and likely masked after the evidence was clipped, two cameras were broken and awaiting repair, and the Department requested that camera technicians apply an additional mask to address the final camera.

RTCC staff noted that some delays in digital masking occur because the task must be performed by a City technician at the camera site. Although policy states masking will be done before installation, any additional masking or adjustments after installation depend on technician availability. OIG will continue to monitor digital masking as the department repairs, replaces, and potentially installs new cameras.

⁸ SPD Policy [12.100-POL-2\(1\)](#).

⁹ SPD reported that digital masking is applied by a City technician at the camera level so that masking cannot be removed to view private areas.

The City Did Not Establish Clear Requirements and Safeguards for Private Cameras

SMC 14.18 governing the acquisition and use of surveillance technologies provides that a Surveillance Impact Report will include:

“How and when the surveillance technology will be deployed or used and by whom, including but not limited to: the factors that will be used to determine where, when, and how the technology is deployed [...]”

OIG found that while both CCTV and RTCC SIRs address integration of privately owned cameras as a future possibility, the reports provide no criteria for deployment.¹⁰ Based on the requirements of SMC 14.18, criteria for private camera integration should at minimum include guidance on where SPD can accept private camera feeds within the city, guidance for retention periods, and restrictions on visibility into non-public spaces.

Location of Private Integrations

A significant and timely question these criteria should answer is whether private cameras are limited to the pilot program areas. Because private camera integration is a feature of both RTCC and CCTV SIRs, it is unclear whether they should be limited to the same areas of the city as the SPD-operated CCTV cameras or integrated citywide like SDOT cameras.

At this time, citywide expansion of private cameras appears neither expressly permitted nor prohibited.¹¹ As such, in August 2026, SPD reported they planned to accept private camera integrations from any business that volunteered, regardless of location within the city.¹² While SPD’s decision does not violate the terms of the SIRs, it is unclear if citywide deployment is consistent with the design of a geographically-limited pilot program.

Privacy Protections

SPD can address privacy concerns related to their own cameras by changing orientation and applying masking, but they do not have the same control of private cameras.

10 As part of the SIR process in 2024, the Community Surveillance Working Group also identified that SPD had not formed a sufficient risk mitigation plan for the integration of private cameras, and that these integrations could lead to uncontained expansion of CCTV coverage.

11 Mayor Wilson’s 2026 directive pausing the expansion of CCTV cameras into three new pilot program areas did not address private cameras.

12 SPD had already integrated two camera locations in Capitol Hill since 2025.

Section 1.1 of the CCTV SIR states:

“In addition to the city-owned and operated CCTV cameras, privately-owned security systems will be able to voluntarily share video of storefronts and areas where the public has access with SPD. This voluntary sharing of CCTV images of publicly accessible areas will increase the effectiveness of the technology-assisted crime prevention effort.”

While viewing public areas is a requirement of the SIR, if the owner of a camera were to move it so that it no longer views public areas, it is up to RTCC staff to notice that change and promptly shut down the feed until the owner corrects the issue.

Though SPD policy states CCTV systems monitored by the RTCC will be oriented to only view spaces open to the public, it does not provide criteria or a process for identifying and remediating cameras that do not meet that standard. Without processes to ensure compliance for private cameras, SPD is at heightened risk of collecting video from non-public or sensitive locations.

Camera Retention

Section 4.1 of the CCTV SIR states that private footage will be subject to 30 days of retention “if used on SPD Storage,” but the SIR does not specify whether Fusus Cores installed on private cameras are part of SPD storage. SPD policy does not make this distinction either, though RTCC staff provided that they do not consider the Cores to be SPD storage because SPD does not own or control them.

Retention settings for private cameras are determined by their owners when installing the Fusus Core and may be set beyond 30 days. While nothing prohibits SPD from receiving video from third parties recorded outside of the Department retention periods, the potential for direct and continual access by RTCC analysts to video of greater than 30 days is not sufficiently addressed in the SIRs or SPD policy.

Recommendation 2: Address Governance Issues Related to Privately Owned Cameras

SPD should, in partnership with City leadership, adopt policies and procedures to specify criteria for integrating privately owned cameras. Criteria should include where they can be used, monitoring and remediation processes, and retention guidelines.

Data Retention, Sharing, and System Access

OIG Identified No Instances of Improperly Shared Data

OIG reviewed user activity logs from both Fusus and Evidence.com for 2025 and found no record of RTCC analysts sharing surveillance data to external entities or allowing non-specified users to access or handle data. Consequently, this review found no indication of improperly shared surveillance data.

SPD received 11 requests for public disclosure related to CCTVs and the RTCC. Requests were related to either a criminal incident or a request for evidence for automobile insurance purposes.

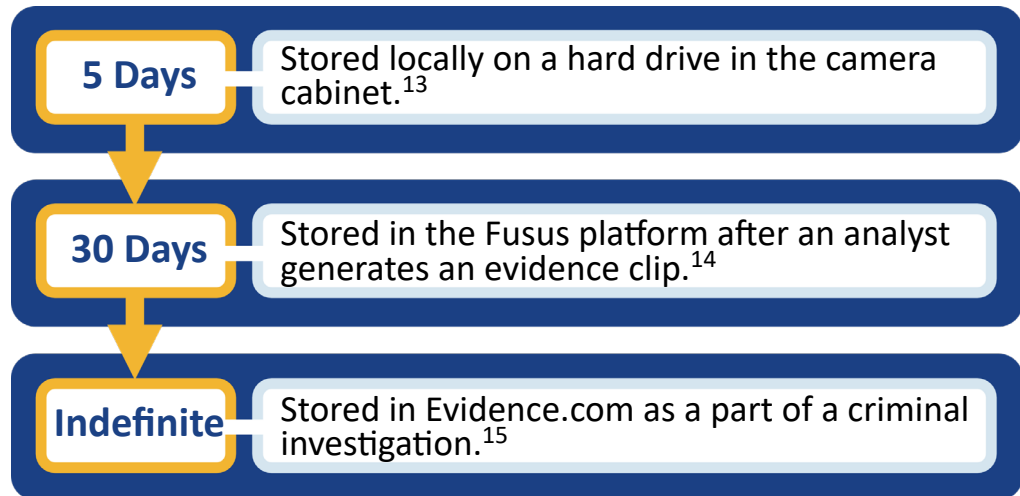
SPD Appropriately Limits Access to Camera Feeds

Axon Fusus is a platform separate from SPD systems. Because of this, only personnel who have an operational need to access the platform have accounts.

OIG observed 31 user accounts in Fusus during 2025. Most users were RTCC personnel and SPD staff involved in technology use or research; other users included administrators from SPD, Seattle Information Technology Department (SITD), and the vendor. OIG identified that all user accounts appear to belong to individuals with an operational need to access the platform.

Implemented Retention Periods Meet SIR Requirements

CCTV data are subject to three different retention periods depending on where it is stored:



OIG conducted a point-in-time review of all evidence in the Fusus platform and confirmed the default retention was set to 30 days. OIG found no recordings retained longer than the 30-day period required by SPD policy.

13 While the CCTV SIR Section 4.1 states that video recordings will not be kept longer than 30 days unless manually extracted by authorized personnel, the RTCC opted to set the retention during 2025 to only 5 days. At the time of this report, that retention period of 5 days has not changed.

14 Section 4.2 of the RTCC SIR states that “Data that is not part of a criminal investigation will be subject to a 30-day retention policy, after which it will be purged from the system.”

15 Evidence in a criminal investigation is controlled by the Washington State Law Enforcement Records Retention Schedule.

Community Concerns and Costs

SMC 14.18 requires OIG to summarize complaints or concerns received or known by departments about the reviewed surveillance technology, as well as the annual costs for the technology.

Community Concerns

OIG searched for complaints filed with the Office of Police Accountability (OPA) complaints or City Customer Service Board (CSB) but did not identify any regarding SPD use of CCTV or RTCC in 2025.

However, CCTV cameras and RTCC have been subjects of ongoing stakeholder and community concern. During the 2024 approval and subsequent expansion of the pilot technologies in 2025, some civil rights and community advocates opposed the use of the technologies expressing concern about risks the technologies could pose to Black and brown communities, immigrant communities, and people seeking reproductive or gender-affirming care. Community members also expressed concern about expanding the pilot technologies during City Council meetings. They noted concerns about civil liberties, federal overreach targeting protected communities, and early expansion of the pilot program.¹⁶

Costs

In 2025, the purchase of camera equipment, installation, and personnel costs amounted to a total of \$3,494,346. Equipment and installation cost account for \$1,445,879 and RTCC personnel costs for \$2,048,467 of the total operational costs in 2025.

¹⁶ The original proposal of the pilot program stated that expansion of the technologies city-wide would occur after an evaluation of effectiveness. That evaluation plan became the basis of the OIG-UPenn collaboration to evaluate the technologies.

Automated License Plate Readers (ALPR)

Read: an image of a license plate number.

Hotlist: a list of license plate numbers associated with criminal incidents compiled from a variety of law enforcement sources.

Unverified Hit: a read that appears to match a criminal record.

Verified Hit: a read that matches a criminal record and has been verified by officers and/or dispatch as a true match.

ALPR Database: a searchable database of reads, unverified hits, and misreads that are retained for 90 days.

ALPR Cameras

Automated License Plate Readers (ALPR) use existing fleetwide in-car camera systems to scan license plates as they come into view. These are known as **reads**. Reads that initially appear to match with an item on a **hotlist** are known as **unverified hits**. SPD policy prohibits officers from acting on unverified hits until they, or dispatch, compare the read and its hotlist match to ensure both the state and characters on the plate match.¹⁷ Officers have discretion whether to act on **verified hits**.

ALPR Database

In addition to the use of ALPR in patrol vehicles, SPD stores license plate reads and data in a searchable database as a resource for investigations. All license plate reads are retained in the **ALPR database** for 90 days, after which they are purged. This database is nested within an existing cloud-based digital evidence management system, Evidence.com. Policy governing searches requires authorized users to provide a case number and a note justifying the nature/purpose of their search. Database users can specify a date range and/or a geographic area when searching reads, unverified hits, or one or more specific license plate(s). The ALPR database provides an audit trail by retaining user activities and search parameters.

ALPR Expansion and Subsequent Pause

In June 2024, the City of Seattle approved the fleetwide expansion of ALPR by SPD. Prior to this expansion, ALPR was limited to 11 patrol vehicles with separately mounted camera systems; after this expansion, those systems were decommissioned and SPD modified its contract with Axon to enable ALPR functioning with existing in-car video cameras.

In March 2026, SPD turned off all ALPR capabilities following passage of State legislation restricting collection, retention, and sharing of license plate data.¹⁸ All records in the database were purged and the database was shut down. The ALPR systems remain inactive at the time of this report. Because these systems were active during the 2025 review period, this report evaluates department usage of both the ALPRs and the ALPR database for that period.

¹⁷ SPD Policy [16.170 POL-2 \(4\)](#).

¹⁸ Senate Bill 6002, termed the Driver Privacy Act.

How SPD Uses ALPRs

Hits Occurred Everywhere, But Were Concentrated in Certain Neighborhoods

Over a nine-month period from April through December 2025, SPD officers recorded 3,346 verified hits in Seattle, with a median number of 49 verified hits per neighborhood.¹⁹ These verified hits included 1,894 unique license plates. Figure 4 illustrates the volume of verified hits distributed across Seattle neighborhoods.

Of the 3,346 verified hits in this period, SPD records indicate that 83 arrests occurred after verifying a hit, 78 of which were reported as felony arrests. Most arrests or criminal charges from a verified hit are associated with hotlist hits for stolen vehicles or license plates.

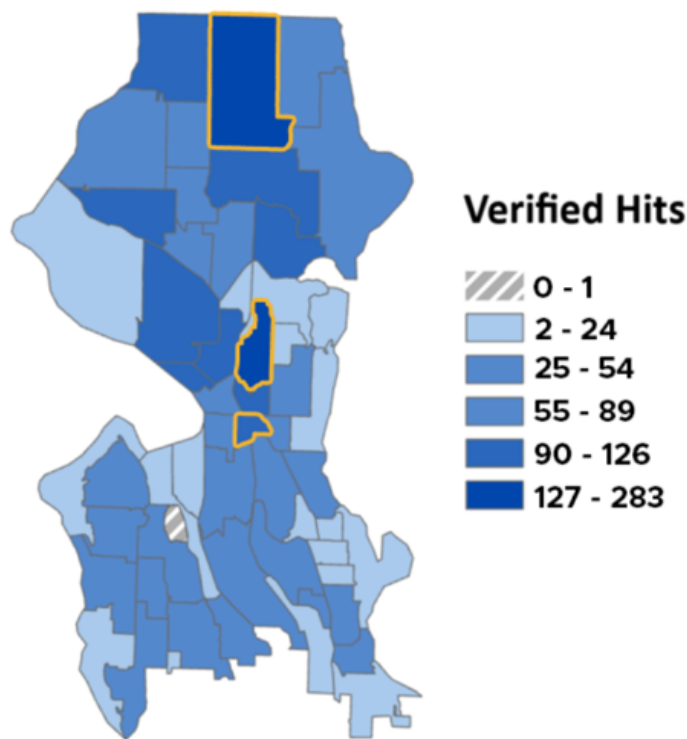


Figure 4: Verified Hits by Seattle Neighborhood

**Since ALPRs can scan the same license plate multiple times during a single interaction, Figure 4 shows an aggregate number of verified hits by individual license plate reads in a single day from April-December of 2025.*

¹⁹ OIG was unable to complete an analysis of unique license plates from January through March prior to SPD lawful purge of the records from this time period.

SPD Excludes Records of Immigration Violators from Hotlists

State law prohibits law enforcement from using agency funds, facilities, property, personnel or equipment to investigate, enforce, cooperate with, or assist investigation or enforcements of any federal registration or surveillance programs solely based on race, religion, immigration or citizenship status, or national or ethnic origin.²⁰

SPD hotlist records are largely derived from the FBI National Crime Information Center database, which may include immigration-related offenses. OIG observed that SPD sets their digital evidence management system to exclude the integration of records associated with civil immigration violations.

Data Retention, Sharing, and System Access

After license plate images are recorded by an ALPR, they are uploaded to the ALPR database. The images are retained for 90 days before being automatically purged. During this 90-day window, certain department staff may search the database for records related to criminal incidents. Whenever these department staff identify records that are potentially related to a criminal incident, they download the records to add them to case investigation files. This sometimes means that the license plate images are then re-uploaded as evidence to Evidence.com (but not in the ALPR database). If ALPR images are retained as evidence, SPD personnel may share these records, provided the sharing adheres to SPD policy and local/state laws.

Record Retention Period Enforcement

SPD policy states that ALPR data will be retained for 90 days, unless “it has become, or it is reasonable to believe it will become, evidence in a criminal or civil action, or is subject to a lawful action to produce records.”²¹

²⁰ RCW 43.17.425 (Keep Washington Working Act).

²¹ SPD [Policy 16.170](#).

OIG found no evidence that read/hit records were retained in the ALPR database longer than 90 days during 2025. While OIG could not assess to what extent downloaded records were appropriately purged or retained, several SPD policies governing the storage and sharing of evidence mitigate risk of accidental mishandling.²²

SPD Appropriately Limits the Number of Users Who Can Access the ALPR Database

SPD policy and the SIR limit ALPR database access to a small number of sworn investigators and civilian analysts. There were more than 1,200 active SPD Evidence.com users in 2025, but only 33 had access to the ALPR database within Evidence.com. Of these 33 users, 29 accessed ALPR data in 2025. OIG reviewed all users' activities in Evidence.com in 2025 and found no instances of unauthorized access to the ALPR database.

To manage user access, SPD administrators create user groups with certain permissions and regularly conduct manual reviews of these groups and any role/privilege changes. For example, any change to job titles impacting database access requires administrators to actively review those changes and update permissions accordingly. Permissions for users differ according to job duties; for example, at the time of review nine users could create custom hotlists: three administrators (civilians), three supervisors (sworn officers), and three investigators (sworn officers). With these access controls, SPD ALPR data access aligns with best practices from National Institute of Standards and Technology (NIST) principle of least privilege.²³

Documentation of ALPR Search Reasons Is Often Insufficient

SPD policy requires employees conducting ALPR database searches to provide a case number and a justification for the search (or if there is no available case number, a justification).²⁴

However users did not provide justifications for approximately 47% of searches in 2025. In prior years, such non-compliance occurred at a rate of

22 SPD policy governs how physical evidence must be submitted/handled (Policies 7.010, 7.030, and 7.040); where digital evidence must be stored (Policy 7.090); which entities can receive physical and digital evidence (Policy 7.010); and how non-criminal justice related parties may be approved to receive physical and digital evidence (Policies 7.010 and 7.060). Numerous sections of the SPD Policy Manual prohibit storage of such copies or original digital evidence on personal devices (e.g., Policies 7.090, 7.110, and 16.170).

23 NIST Special Publication 800-12 Rev. 1 defines Least Privilege as "The principle that a security architecture should be designed so that each entity is granted the minimum system resources and authorizations that the entity needs to perform its function."

24 SPD Policy [16.170 POL-6](#).

37% (2023) and 24% (2024). The previous ALPR user interface required users to either 1) provide a case number and select a justification from a drop-down menu or 2) provide text in a note field (which conformed with policy at the time).

While OIG found that case numbers were generally provided for reviewed searches in 2025, there is no current process for validating these case numbers with SPD records or case numbers from other jurisdictions. Without proper justification accompanied by a case number, a review of user activity may be unable to determine whether specific access was proper.

Recommendation 3: Ensure Department Searches Align with SPD Policy

SPD should design and implement a process to ensure authorized users of the ALPR database provide both a search justification and case number as required in SPD policy.

SPD Personnel Report They Exercise Caution in Sharing ALPR Data Externally

SPD can share ALPR records with partner agencies such as the City Attorney's Office, King County Sheriff's Office, or the King County Prosecuting Attorney's Office by generating a link in Evidence.com. Sharing through Evidence.com is tracked for every record. Less frequently, SPD personnel share evidence with an external partner who does not use Evidence.com. In such cases, SPD personnel transmit the evidence by another medium such as email.

Regardless of the sharing method, SPD personnel must first download the ALPR image or data from the ALPR database within Evidence.com.²⁵ Not all downloaded files must be shared, but OIG found that in 2025, 26 authorized users downloaded 1,223 license plate number (LPN) image files of reads/hits, and 13 users downloaded 71 CSV files containing read/hit record data. OIG interviewed several of these users about the purposes of these downloads and practices for sharing.²⁶

²⁵ Though the ALPR database is located within Evidence.com, the images it contains are not stored as evidence; consequently, sharing cannot occur directly out of the ALPR database. To share ALPR images as evidence through Evidence.com, the images must be added to the digital case file, which requires re-upload.

²⁶ A mixture of sworn investigators and civilian analysts comprised the authorized users who downloaded records.

Users reported they rarely shared these data with other jurisdictions (local or federal) outside of Evidence.com, and that any data sharing was pursuant to a legitimate criminal investigation, in compliance with SPD policy and local and state laws. These users reported that record sharing with federal agencies – generally through participation on a task force – only occurred after confirming their support was not involved in investigating or enforcing immigration or documentation status.

Vendor Data Sharing Remains a Potential Risk

SPD is required by ordinance to immediately pause ALPR data collection for 60 days if the City or its vendor, Axon, receive a warrant, subpoena, court order, or is otherwise required to release ALPR data for use in a civil immigration enforcement or a criminal case for accessing healthcare prohibited in other states: gender affirming care or reproductive care.²⁷

Because SPD deactivated ALPR systems until they can configure systems to comply with Washington State Driver Privacy Act, the risk to vendor-held data is temporarily averted. However, when SPD reactivates ALPR systems, it will be necessary for the City to understand Axon policies and practices regarding ALPR data sharing and plan accordingly. OIG is aware of a separate review conducted by the Mayor's Office currently seeking to address this issue, and OIG awaits those findings.

Public Disclosure Requests

During this period SPD filled one request related to SPD use of ALPR. This request did not require SPD to disclose any data gathered by ALPR.

²⁷ City of Seattle Ordinance 127412.

Community Concerns and Costs

SMC 14.18 requires OIG to summarize complaints or concerns received or known by departments about the reviewed surveillance technology, as well as the annual costs for the technology.

Community Concerns

OIG searched for complaints filed with the Office of Police Accountability (OPA) complaints or City Customer Service Board (CSB) but did not identify any regarding SPD use of ALPR in 2025.

Like CCTV cameras and RTCC, ALPR has been the subject of ongoing community concerns about civil liberties, external entities targeting protected communities, and premature expansion of the pilot program.

Costs

In November of 2024, SPD signed a 54-month contract with Axon to expand ALPR to fleetwide for a total of \$1,401,716.55. The total cost for attributed in 2025 was \$268,511.

Non-Audit Statement This review was not conducted under Generally Accepted Government Auditing Standards (GAGAS); however, OIG has followed GAGAS standards regarding the sufficiency and appropriateness of evidence.

SPD Management Recommendations Response

Recommendation 1: Implement Additional Access Controls for Viewing CCTV Feeds

SPD should request Axon implement a requirement for RTCC analysts to provide a case number and/or justification for each instance they view CCTV camera footage in the Axon Fusus software.

SPD Management Response

☒ Concur ☐ Do Not Concur

Estimated Date of Implementation: October 16, 2026

Proposed Implementation Plan: Proposed Implementation Plan: SPD has already requested this feature as an enhancement for Fusus but will submit a formal request by the date listed above.

Recommendation 2: Address Governance Issues Related to Privately Owned Cameras

SPD should, in partnership with City leadership, adopt policies and procedures to specify criteria for integrating privately owned cameras. Criteria should include where they can be used, monitoring and remediation processes, and retention guidelines.

SPD Management Response

☒ Concur ☐ Do Not Concur

Estimated Date of Implementation: March 15th, 2027

Proposed Implementation Plan: As part of an Omnibus Surveillance Policy, SPD will propose policy to clarify access and locations for privately integrated cameras. The policy will propose restricting access to historical footage to align with public cameras (five days with no proactive live monitoring), restrict ingestion of private camera feeds to only include public areas, and allow for private camera feeds city-wide. In addition, the policy will propose procedures to do regular checks and internal audits of private cameras to help ensure compliance.

Recommendation 3: Ensure Department Searches Align with SPD Policy

SPD should design and implement a process to ensure authorized users of the ALPR database provide both a search justification and case number as required in SPD policy.

SPD Management Response

☒ Concur ☐ Do Not Concur

Proposed Implementation Plan: First and foremost, SPD is currently on pause with ALPR systems in both patrol and parking enforcement areas to ensure compliance with new State law.

Currently, there is a justification field that is required before a search is made. It is also in SPD policy (16.170 POL 6 Section 2) that “Employees Conducting Searches in the Patrol ALPR System Will Provide a Case Number and Justification for the Search. If a case number does not exist, the employees will provide thorough justification for the legitimacy and lawful purpose of the search.” SPD will develop internal procedures re-enforcing the SPD policy, as well as conduct training to ensure compliance with policy by the date above.

In addition, SPD will engage with the ALPR vendors to include both a required case number and justification field.